

CLAIMS

1-50. (cancelled)

51. (currently amended) A method of thwarting detection of a secret binary number in a cryptographic computational device by analysis of externally observable parameters, comprising:

conditionally performing a plurality of calculations in response to the bit values of  
said secret number;

multiplicatively accumulating the results of said plurality of calculations in a  
subtotal; and

performing dummy calculations in response to selected bit positions of said  
secret number that indicate calculations should not be performed, and not  
multiplicatively accumulating the results of the dummy calculations in said  
subtotal, said selected bit positions randomly distributed over a binary  
indicator equal in length to said secret number;

whereby said dummy calculations alter at least one externally observable  
parameter.

52. (previously presented) The method of claim 51 wherein conditionally performing a plurality of calculations in response to the bit values of said secret number comprises performing a calculation where said bit value is a one and not performing said calculation where said bit value is a zero.

53. (currently amended) The method of claim 52 wherein performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed comprises performing said dummy calculations in

response to ~~selected ones of~~ said secret number bit positions ~~whose bit value is being a~~  
zero and a corresponding indicator bit position being a one.

54-55. (cancelled)

56. (previously presented) The method of claim 53 wherein said indicator is fixed.

57. (currently amended) The method of claim 56 wherein said indicator is generated upon first commissioning said device into operation and internally ~~storing said indicator~~ stored such that it is never released outside said device.

58. (previously presented) The method of claim 51 further comprising generating said secret number upon first commissioning said device into operation and internally storing said secret number such that it is never released outside said device.

59. (previously presented) The method of claim 51 in which said externally observable parameters include variation in power supply current.

60. (previously presented) The method of claim 51 in which said externally observable parameters include variation in timing of outputting results of said calculations.

61. (previously presented) The method of claim 51 wherein conditionally performing a plurality of calculations and accumulating their results calculates the exponentiation of a long integer to the power of a large secret exponent.

62. (previously presented) The method of claim 61 in which calculating the exponentiation of a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

63. (currently amended) A method of thwarting detection of a large, secret binary exponent in a cryptographic computational device executing the operation of exponentiating a long integer to the power of said secret exponent, the detection being by analysis of externally observable parameters of said device, comprising:

calculating successive squares of said long integer in a group of a predetermined size and temporarily storing the results, each said square calculated by either a square operation or a multiply operation in response to a predetermined, random indicator, said square and multiply operations ~~calculations~~ altering at least one said externally observable parameter; and

multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent, said selection of results to be accumulated not substantially altering an externally observable parameter.

64. (previously presented) The method of claim 63 wherein selectively multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent comprises multiplicatively accumulating each said result if the corresponding bit value of said secret

exponent is a one, and not multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a zero.

65. (previously presented) The method of claim 63 wherein said predetermined size is the bit length of said secret binary exponent.

66. (previously presented) The method of claim 63 further comprising recalculating each said successive square in said group, regardless of whether said square was multiplicatively accumulated, using values for the corresponding successive square of the next said group of bit values.

67-72. (cancelled)

73. (currently amended) A detection-proof computational device comprising:  
an input/output interface;  
a memory storing a secret binary number; and  
a processor operatively connected to said input/output interface and to said memory and programmed for cryptographic computation using said secret binary number while thwarting detection of said secret binary number by analysis of externally observable parameters, the cryptographic computation comprising:  
conditionally performing a plurality of calculations in response to the bit values of said secret number;  
multiplicatively accumulating the results of said plurality of calculations in a subtotal; and

performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed, and not multiplicatively accumulating the results of the dummy calculations in said subtotal, said selected bit positions randomly distributed over a binary indicator equal in length to said secret number;  
whereby said dummy calculations alter at least one externally observable parameter.

74-75. (cancelled)

76. (previously presented) The device of claim 73 in which in which said externally observable parameters include variation in power supply current.

77. (previously presented) The device of claim 73 in which said externally observable parameters include variation in timing of outputting results of said calculations.

78. (previously presented) The device of claim 73 wherein said secret cryptographic computations comprise exponentiating a long integer to the power of a large secret exponent.

79. (previously presented) The device of claim 78 wherein exponentiating a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

80. (currently amended) A secure computational device comprising:

- an input/output interface receiving a long integer;
- a memory storing a secret exponent; and
- a processor operatively connected to said input/output interface and to said memory and programmed for the cryptographic computation of exponentiating said long integer to the power of said secret exponent, while thwarting detection of said secret exponent by analysis of externally observable parameters, the cryptographic computation comprising:
  - calculating successive squares of said long integer in a group of a predetermined size and temporarily storing the results, each said square calculated by either a square operation or a multiply operation in response to a predetermined, random indicator, said square and multiply operations ~~calculations~~ altering at least one said externally observable parameter; and
  - multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent, said selection of results to be accumulated not substantially altering an externally observable parameter.

81. (previously presented) The device of claim 80 wherein selectively multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent comprises multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a

one, and not multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a zero.

82. (previously presented) The device of claim 80 wherein said predetermined size is the bit length of said secret binary exponent.

83. (currently amended) The device of claim 80 ~~further~~ wherein said processor further recalculates each said successive square in said group, regardless of whether said square was multiplicatively accumulated, using values for the corresponding successive square of the next said group of bit values.

84. (previously presented) The device of claim 80 wherein said device comprises a smart card.

85-87. (cancelled)

88. (currently amended) A mobile terminal used in a mobile communications system comprising:

- a transmitter and a receiver for communicating in the mobile communications system;

- a controller controlling operation of the transmitter and the receiver; and

- a secure device removably, operatively connectable to the controller and comprising:

- an input/output interface;

- a memory storing a secret binary number; and

a processor operatively connected to said input/output interface and to  
said memory and programmed for cryptographic computation  
using said secret binary number while thwarting detection of said  
secret binary number by analysis of externally observable  
parameters, the cryptographic computation comprising:  
conditionally performing a plurality of calculations in response to  
the bit values of said secret number;  
multiplicatively accumulating the results of said plurality of  
calculations in a subtotal; and  
performing dummy calculations in response to selected bit  
positions of said secret number that indicate calculations  
should not be performed, and not multiplicatively  
accumulating the results of the dummy calculations in said  
subtotal, said selected bit positions randomly distributed  
over a binary indicator equal in length to said secret  
number;  
whereby said dummy calculations alter at least one externally  
observable parameter.

89-90. (cancelled)

91. (previously presented) The mobile terminal of claim 88 in which in which said  
externally observable parameters include variation in power supply current.

92. (previously presented) The mobile terminal of claim 88 in which said externally observable parameters include variation in timing of outputting results of said calculations.
93. (previously presented) The mobile terminal of claim 88 wherein said secret cryptographic computations comprise exponentiating a long integer to the power of a large secret exponent.
94. (previously presented) The mobile terminal of claim 93 wherein exponentiating a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.
95. (currently amended) A mobile terminal used in a mobile communications system comprising:
- a transmitter and a receiver for communicating in the mobile communications system;
  - a controller controlling operation of the transmitter and the receiver; and
  - a secure device removably, operatively connectable to the controller and comprising:
    - an input/output interface receiving a long integer;
    - a memory storing a secret exponent; and
    - a processor operatively connected to said input/output interface and to said memory and programmed for the cryptographic computation of exponentiating said long integer to the power of said secret

exponent, while thwarting detection of said secret exponent by analysis of externally observable parameters, the cryptographic computation comprising:

calculating successive squares of said long integer in a group of a

predetermined size and temporarily storing the results,

each said square calculated by either a square operation

or a multiply operation in response to a predetermined,

random indicator, said square and multiply operations

calculations altering at least one said externally observable parameter; and

multiplicatively accumulating selected ones of the results of said

plurality of calculations in response to a corresponding

group of bit values of said secret exponent, said selection

of results to be accumulated not substantially altering an

externally observable parameter.

96. (previously presented) The mobile terminal of claim 95 wherein selectively multiplicatively accumulating selected ones of the results of said plurality of calculations in response to a corresponding group of bit values of said secret exponent comprises multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a one, and not multiplicatively accumulating each said result if the corresponding bit value of said secret exponent is a zero.

97. (previously presented) The mobile terminal of claim 95 wherein said predetermined size is the bit length of said secret binary exponent.

98. (previously presented) The mobile terminal of claim 95 wherein said processor further recalculates each said successive square in said group, regardless of whether said square was multiplicatively accumulated, using values for the corresponding successive square of the next said group of bit values.

99-103. (cancelled)

104. (new) The method of claim 63 wherein said predetermined size is eight bits.

105. (new) The device of claim 80 wherein said predetermined size is eight bits.

106. (new) The mobile terminal of claim 95 wherein said predetermined size is eight bits.